

3/4/02

**SUBJ: INTERNET SERVICES**

---

- 1. PURPOSE.** This order assigns organizational and management responsibilities for Internet services to conform to security and privacy considerations. This order facilitates the effective oversight of Internet services and defines an authorization process based on a registration process that incorporates a privacy review and a security practice agreement.
- 2. DISTRIBUTION.** This order is distributed to the division level in Washington headquarters, regions, and centers with a limited distribution to all facilities and field offices.
- 3. SCOPE.** This order applies to the provision of Internet services to all offices, services, regions, centers, employees, contractors, and support personnel who use or operate FAA-owned and FAA-funded systems, applications, data, and information. Internet services include, but are not limited to, file transfer, remote login access, Wide Area Information Server (WAIS), websites, and established electronic discussion groups available to employees, contractor support personnel, consultants, etc., using FAA-owned and FAA-funded computing or network resources.

**4. BACKGROUND.**

a. On February 22, 2000, AIO-1 issued a memorandum entitled, Securing FAA Websites. This memorandum established preliminary security guidelines to be instituted on all computers whether for administrative use, National Airspace System (NAS) support, or NAS operations to increase security of all FAA websites. Guidance for drafting the memorandum was taken from Department of Transportation (DOT) Handbook, DOT H 1350.2, Departmental Information Resources Management Manual (DIRMM), Chapter 14-4, DOT Internet Policy. The DOT initially established security guidelines and published them in DOT H 1350.2 to address the security risks associated with increased usage of the Internet. On June 9, 2000, Order 1370.82, Information Systems Security Program, was signed by the Administrator authorizing the Assistant Administrator for Information Services (AIO-1) to issue detailed information systems security (ISS) implementation orders, procedures, and guidance. Order 1370.82 mandates that all FAA personnel, contractors, and subcontractors working for, on behalf of, or connected to FAA systems take security measures commensurate with the sensitivity level of the information. In an effort to fulfill the security requirements of 1370.82 and DOT H 1350.2 with respect to Internet services, each line of business (LOB) or staff office (SO) will apply security practice agreements to all FAA Internet services.

b. This order also addresses concerns about individual privacy when using FAA Internet services. General concerns about privacy are addressed in the Electronic Access Privacy and Security Statement in Appendix 3 of this order. This order also addresses some of the FAA's obligations under the Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988, and Order 1280.1, Protecting Privacy of Information About Individuals. This order specifically prohibits the unauthorized use of methods that collect user-identifying information on individual visitors to publicly accessible Internet services to identify or build profiles, e.g., extensive lists of previously visited sites, e-mail addresses, or other information. In addition, this order defines a privacy review to be completed by each LOB/SO for all FAA Internet services.

c. This order establishes a registration process for Internet services and assigns the Chief Information Officer (CIO) or Information Resource Manager (IRM) for each LOB/SO as the registrar for their respective LOB/SO. The registration of Internet services will allow for the successful monitoring of services for compliance with pertinent laws, allow for effective inventory management, expedite responding to requests for information regarding FAA Internet services, and make it easier

to inform LOB/SOs when security, privacy, registration, or other changes to laws and ISS requirements occur. The registration of the Internet service will include the privacy review and a security practice agreement.

**5. DEFINITIONS.** Appendix 1, Definitions, defines the terms used in this order.

**6. POLICY IMPLEMENTATION.** The FAA shall ensure that active measures to protect the privacy of individuals are taken on all FAA Internet services accessible by the public and will ensure the security of information resident on the servers. The FAA will enact a registration process for Internet services to allow for appropriate monitoring. LOB/SOs will register and authorize Internet services based on a privacy review and a security practice agreement described in this order. Wording in Appendix 2, Standard Notification When Leaving an FAA Internet service, and Appendix 3, Electronic Access Privacy and Security Statement, may be changed by AIO-1 in coordination with legal counsel.

**a. Privacy** – The FAA will take measures to comply with its Electronic Access Privacy and Security Statement (Appendix 3) and the Privacy Act. All Internet services must undergo a privacy review prior to being registered. The results of the privacy review must be documented and included with the registration information.

(1) Each webmaster shall display a link to the Electronic Access Privacy and Security Statement, which appears in Appendix 3, on all FAA domain level homepages and on all FAA webpages where personal information is collected from the public. In addition, the webmaster shall notify users that they are no longer protected under FAA privacy policies when they leave FAA websites (Appendix 3).

(2) The FAA will not collect, maintain, or use information about an individual that is retrieved by their name or personal identifier unless the FAA publishes a notice establishing a System of Records in the Federal Register in accordance with the Privacy Act. Any technical means for collecting and maintaining information from individuals must be approved by AIO-1 prior to operation. If a technical means for collecting and maintaining information about individuals is approved by AIO-1, then the appropriate procedures for establishing a Privacy Act System of Records must be established through the Standards and Information Division (APF-100) in the Office of Cost and Performance Management.

(3) With respect to the collection of information obtained from the public through e-mail or web forms, FAA organizations are prohibited from collecting, maintaining, using, or disseminating such information until they determine whether the activity is subject to the Privacy Act. Accordingly, FAA organizations shall not invite and/or encourage the public to access their site(s) until this determination is made. Information received from the public and stored by the FAA that is not retrieved by name or personal identifier is not subject to the Privacy Act (e.g., e-mails requesting corrections to the website).

(4) The manager of the content provider is responsible for conducting a privacy review prior to posting information for a LOB/SO in an effort to ensure the security and confidentiality of any personal information or information covered under the Privacy Act.

(5) In addition to administrative actions within the FAA, violators of the Privacy Act are subject to civil and criminal penalties as specified in 5 U.S.C. 552a.

(6) The designated approving authority (DAA) for each LOB/SO has the authority to disconnect an Internet service for their respective LOB/SO until the Internet service comes into compliance with the privacy requirements addressed in this order.

**b. Security** – The FAA will ensure that security requirements are developed and applied, throughout the lifecycle, to protect information systems that are available to the public. Internet services must meet the security requirements expressed in Order 1370.79, Internet Use Policy; Order 1370.82, Information Systems Security Program; and Order 1370.83, Internet Access Points. The manager of the content provider has primary responsibility for ensuring their Internet services comply with this order. The manager of the content provider, in conjunction with the LOB/SO information systems security manager (ISSM), will prepare a security practice agreement that describes the Internet service and the management, operational, and technical controls in place to protect the service. All Internet services must operate on certified servers. Existing services will either move to a certified server or have the existing server complete the certification and authorization process defined in Order 1370.82 within one year of the approval date of this order. Servers can be certified individually or as part of a system. After one year from the approval date of this order, the DAA for the LOB/SO will disconnect Internet services operating on uncertified servers.

For existing certified systems, the system owner, in conjunction with the ISSM for the system, will determine if changes need to be made to the System Certification Authorization Package (SCAP). The DAA for each LOB/SO has the authority to disconnect an Internet service until the service comes into compliance with the security requirements addressed in this order. At a minimum, each LOB/SO will establish and utilize appropriate security procedures and conduct security audits to ensure system operation and data integrity. The security practice agreement will be based on industry best practices and its format must be approved by AIO-1. At a minimum, the security practice agreement will:

- (1) Be completed before the Internet service becomes operational. Security Practice Agreements for existing services will be completed within 180 days of approval date of this order.
- (2) Provide user authentication for authorized users wishing to establish a connection with FAA internal computers via the Internet.
- (3) Ensure that FAA Internet servers and any data to be accessed by the general public are separated from the FAA internal network.
- (4) Explicitly state if a SCAP will be prepared to certify and authorize the Internet service. The LOB/SO ISSM will determine if a SCAP is required. If a SCAP is required, it must be approved by the associated DAA.
- (5) Address Internet services provided by contract and verify that the implementation of security requirements is documented in the contract and statement of work. The acquiring organization will be responsible for ensuring compliance with those requirements in accordance with FAA orders (e.g. Order 1600.1D, Personnel Security Program) and the Acquisitions Managements System (AMS).
- (6) Ensure users are notified of FAA security policies by displaying a link to the Electronic Access Privacy and Security Statement for all FAA domain level homepages and on all FAA web pages where personal information is collected from the public (Appendix 3). The FAA Electronic Access Privacy and Security Statement in Appendix 3 addresses monitoring and logging for statistics, accountability, and forensic purposes. All web pages that require users to log-in shall have a banner conforming to Order 1370.79 warning banner guidance or an alternate banner approved in writing by AIO-1 and legal counsel.
- (7) Authorize the Computer Security Incident Response Center (CSIRC) to terminate Internet access to Internet services in time-critical situations, e.g., CODE RED worm.

**c. Registration** – Each LOB/SO may establish a process, equivalent to the one described, with unique or additional roles and responsibilities to accomplish the registration requirements of this section. The manager of the content provider must register their Internet service with their LOB/SO CIO or IRM within 180 days of approval date of this order and annually thereafter. The manager of the content provider should obtain technical information from the system owner to complete the registration, e.g., associated system SCAP date. The registration will include the results of the privacy review and a completed security practice agreement. The registrar will approve or disapprove an Internet service based on compliance with applicable security, privacy, and other laws and requirements. Each LOB/SO may establish additional requirements based on their LOB/SO needs. The DAA for each LOB/SO has the authority to disconnect an Internet service until the service comes into compliance with the requirements of this order.

- (1) Existing Internet services may be registered prior to completing an Internet service SCAP or associated system SCAP.
- (2) New Internet services shall be registered prior to going online.
- (3) The registrar of the Internet service shall forward all registration information electronically to the Office of Information Systems Security, Resource and Data Management Division (AIS-100). The registration information will be protected as sensitive and properly marked. Besides annual submission, the registrar shall forward new and changed information to AIS-100 as soon as it is received
- (4) The CIO or IRM for the LOB/SO shall also maintain a consolidated list of their Internet services. An updated list will be electronically forwarded to AIS-100 with each registration submission. The consolidated information will include:

- (a) Common name of the Internet service (e.g., FAA homepage).
- (b) Top level uniform resource indicator/uniform resource locator (e.g., [www.faa.gov](http://www.faa.gov)).
- (c) Associated system SCAP date or projected SCAP completion date coordinated with the Office of Information Systems Security, Certification and Compliance Division (AIS-300), in conjunction with the system owner.
- (d) Manager of the content provider contact information:
  - 1. FAA e-mail address
  - 2. Organization
  - 3. Office phone number

7. **WAIVERS.** Requests for exceptions to any portion of this order shall be submitted to AIO-1.

8. **ROLES AND RESPONSIBILITIES.** The roles and responsibilities for FAA Internet services are interpreted under Order 1370.82.

**a. Office of Information Services and Chief Information Officer (AIO).**

(1) The Assistant Administrator for Information Services and Chief Information Officer (AIO-1):

- (a) Issues waivers.
- (b) Tracks new and existing Internet services.
- (c) Approves the security practice agreement template.

(2) The Director of Information Systems Security (AIS-1):

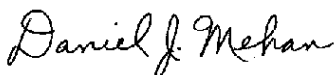
- (a) Develops agency Internet services security policy and guidance. This specifically includes developing guidance on tailoring the certification process to significantly reduce the resources required to prepare a SCAP on servers that are independent of other systems, e.g., some LOB/SO web servers.
- (b) Reviews SCAPs presented by owners of Internet services.
- (c) Audits security compliance.
- (d) Audits privacy compliance in conjunction with APF-100.
- (e) Receives and manages registration information submitted from LOB/SO.

**b. LOB/SO.** Responsible for implementing this policy within their respective organizations, including delegating authority and holding delegates (e.g., network administrators, ISSMs, content managers, web designers, webmasters, etc.) accountable for their actions.

(1) The CIO or IRM:

- (a) Serves as the Internet services registrar and maintains a consolidated list of registration information.
- (b) Approves and disapproves an Internet service based on a privacy review and the security practice agreement.

- (c) Submits registration information to AIS-100.
- (2) The System Owner:
  - (a) Hosts the Internet service.
  - (b) Updates system SCAP in conjunction with the ISSM.
  - (c) Decides if the system needs a new SCAP in conjunction with the ISSM.
- (3) The ISSM:
  - (a) Reviews the system SCAP and advises the DAA whether or not to authorize the system.
  - (b) Updates system SCAP in conjunction with the system owner.
  - (c) Decides if the system needs a SCAP in conjunction with the system owner.
  - (d) Oversees and assists in the creation of the security practice agreements. Reviews the security practice agreements prior to registration.
  - (e) May conduct security audits of LOB/SO Internet Services for compliance with the security practice agreement.
- (4) The DAA:
  - (a) Approves the system SCAP.
  - (b) Authorizes the disconnection of Internet services not in compliance with this order.
  - (c) Makes immediate notification to AIO when an Internet service is disconnected because of noncompliance with any part of this order.
- (5) The Manager of the Content Provider:
  - (a) Prepares the security practice agreement.
  - (b) Ensures the Internet service continues to comply with the security practice agreement.
  - (c) Approves the posting of information on an Internet service within the controls of the security practice agreement.
  - (d) Conducts a content review for compliance with privacy requirements.
  - (e) Ensures the Internet service complies with privacy policies in conjunction with APF-100.
  - (f) Registers new and existing Internet services with the LOB/SO registrar.
  - (g) Ensures the Internet service complies with ISS policies.



Daniel J. Mehan  
Assistant Administrator for Information Services  
and Chief Information Officer



## APPENDIX 1. DEFINITIONS

**Accountability.** Holding people responsible for their actions.

**Content Provider.** The person who supplies information to be posted on an Internet service. The content provider may provide the information directly to the system owner or indirectly through the webmaster.

**Internet.** A global public network of independent hosts and communications facilities, which connect users to those hosts. The term "Internet" also may refer to the content presented on the hosts or transmitted through the network. The FAA may contribute information and resources to the Internet for public consumption.

**Internet Protocol (IP).** The standards by which computers talk to other computers via the Internet.

**IP Address.** A number that identifies a computer that is linked to the Internet. When displayed, an IP address is typically written as four numbers separated by periods (e.g., 24.12.33.56).

**Internet Services.** Services offered by the FAA to the public for exchanging information. These services include but are not limited to webpages, file transfer, remote log-in access, WAIS, websites, and established electronic discussion groups available to employees, contractor support personnel, consultants, etc., using FAA-owned and FAA-funded computing or network resources.

**Manager of the Content Provider.** A government employee with supervisory responsibilities for the content provider. For contract personnel, the manager of the content provider is the contracting officer's technical representative (COTR).

**Privacy Act System of Records.** A group of any "records," as the term is defined in the Privacy Act, under FAA control from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act defines a "record" as any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, their education, financial transactions, medical history, and criminal or employment history, that contains their name or the identifying number, symbol, or other identifying particular assigned to the individual.

**Privacy Review.** A review conducted by the manager of the content provider to ensure information provided to an Internet service is not regulated by the Privacy Act. This review must be conducted prior to providing information through an Internet service.

**Public.** Non-FAA entities.

**Registration.** An approval process that must be conducted on each existing Internet service to continue operation. New Internet service must be registered prior to going online. The required process of formally identifying Internet services to the LOB/SO CIO or IRM that ensures that all security and privacy concerns have been addressed.

**Security Audit.** An audit of the security configuration on the Internet service. The audit assesses the Internet service's compliance with its Security Practice Agreement.

**Security Certification and Authorization Package (SCAP).** The package presented to the Designated Approving Authority for final authorization of a system.

**Security Practice Agreement.** An description of the security configuration on the Internet service. The agreement's format is established by each LOB/SO and is based on industry best practices. The agreement's format is approved by AIO-1 prior to implementation. The agreement must include minimum guidelines as stated in paragraph 6.b.1-7 of this order.

**Server.** A system that provides network service such as disk storage and file transfer or the program that provides such a service for the requestor.

**System.** An assembly of computer hardware, software, or firmware configured for the purpose of classifying, sorting, calculating, computing, summarizing, transmitting and receiving, sorting, or controlling information with a minimum of human intervention.

**System Owner.** The manager responsible for the organization that sets policy, direction, and manages funds for an information system; i.e., owns the system. Systems under development are owned by the developing organization until accepted and authorized by the operating organization. The system owner provides a system to host applications on.

**Uniform Resource Identifier (URI).** The generic term for all types of names and addresses that refer to objects on the World Wide Web. A uniform resource locator is one kind of URI.

**Uniform Resource Locator (URL).** The path descriptor to a specific network resource and the protocol used to access it; e.g., [www.faa.gov/](http://www.faa.gov/). The global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or the domain name where the resource is located.

**Webpage.** A hypertext markup language document containing information that can be seen on the Internet and is identified by a unique URL.

**Website.** A group of webpages under the control of a single organization or individual that have been developed together to present information on a specific subject.

**Webmaster.** An individual who manages a website.



**APPENDIX 2. STANDARD NOTIFICATION WHEN LEAVING AN FAA INTERNET SERVICE**

Our websites have many links to other organizations, such as state/local governments, educational institutions, and non-profit associations. While we offer these electronic linkages for your convenience in accessing transportation-related information, please be aware that when you exit FAA websites, the privacy policy stated on our websites may NOT be the same as that on other websites. You are encouraged to read the privacy policy for each site that you choose to visit.



### **APPENDIX 3. ELECTRONIC ACCESS PRIVACY AND SECURITY STATEMENT**

At the FAA, we recognize the importance of privacy to our website visitors. This privacy policy explains what type of information is collected from you when you visit and how the FAA uses it. For security purposes, this site is subject to monitoring. For more information, see the "Security and Monitoring" section of this statement.

#### ***- INFORMATION COLLECTED AND STORED AUTOMATICALLY***

When you visit the FAA website, we use automated tools to log information about each visit. We process this information in the aggregate to determine site performance issues, such as popular pages, most frequently downloaded forms, and other site performance characteristics. This information does not identify you personally. We do not track or record information about individuals and their visits. The specific data we collect are:

1. The Internet domain (example: www.columbia.edu) and the assigned Internet protocol (IP) address (a number that is assigned to your computer when you are surfing the web).
2. The type of browser and operating system used to access our site.
3. The date and time you access our site.
4. The pages that are viewed and paths that are taken through the website.

These aggregated log data are processed by software tools. The raw log data are retained for three months and are then destroyed.

#### ***- PUBLIC FORUMS***

This site may provide chat rooms, forums, message boards, and e-mail discussion groups to its users. Please remember that any information that is disclosed in these areas becomes public information, and you should exercise caution when deciding to disclose your personal information.

#### ***- ABOUT WEB "COOKIES"***

On some FAA webpages, "session cookies" are utilized to enhance and improve your visit. "Session cookies" expire when you close your web browser. On those webpages that use "persistent cookies," an advisory is posted on that page informing you what information is being collected, why it is being collected, and how it is being used.

#### ***- INFORMATION COLLECTED FROM E-MAIL AND WEB FORMS***

You can contact us by postal mail, telephone, or electronically via an online form. Please do not send information that you would not want a third party to read. For example, please do not send your social security number or credit card information, as it is unlikely these data are needed to respond to your e-mail. The FAA may share the information that you provide to us via e-mail within the agency to respond to your queries, but we do not provide e-mail information to anyone within the agency unless required by law to do so. We will not collect or sell your information for commercial purposes.

#### ***- LINKS TO OTHER SITES***

Our website has links to many other federal agencies. In a few cases we link to private organizations. Once you link to another site, you are subject to the privacy policy of the new site. This website and the information it contains are provided as a public service by the FAA.

#### ***- SECURITY AND MONITORING***

This system is monitored to ensure proper operation, to verify the functioning of applicable security features, possible future forensics, and for comparable purposes. Anyone using this system expressly consents to these activities. Unauthorized attempts to modify any information stored on this system, to defeat or circumvent security features, or to utilize this system for other than its intended purposes are prohibited and may result in criminal prosecution.

#### ***- RESTRICTION OF LIABILITY***

The FAA makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the contents of this website and expressly disclaims liability for errors and omissions in the contents of this website. No warranty of any kind, implied, expressed, or statutory, including but not limited to warranties of non-infringement of third party rights, title, merchantability, fitness for a particular purpose, and freedom from computer virus, is given with respect to the contents of

this website or its hyperlinks to other Internet resources. Reference in this website to any specific commercial products, processes, or services, or the use of any trade, firm, or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation, or favoring by the FAA.

**- OWNERSHIP**

Information presented on this website is considered public information and may be distributed or copied. The FAA shall have the unlimited right to use for any purpose, free of any charge, all information submitted to FAA via this site except those submissions made under separate legal contract. The FAA shall be free to use, for any purpose, any ideas, concepts, or techniques contained in information provided to FAA through this site.